GetLongPathName

Carefully manage buffer sizes

Sean Barnum, Cigital, Inc. [vita[1]]

2007-03-23

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 6179 bytes

Attack Category	• Path spoofing or confusion problem
Vulnerability Category	• Buffer Management • Indeterminate File/Path
Software Context	• File Path Management
Location	• winbase.h
Description	The return buffer for GetLongPathName() and similar functions might return a truncated path and lead to hard-to-find errors. The GetLongPathName() or GetShortPathName() function converts a path to its long or short form. If the lpszLongPath or lpszShortPath buffer is too small to contain the path, the return value is the size of the buffer, in TCHARs, required to hold the path. Call the function again with the proper sized buffer to retrieve the data. The ASCII versions of these functions limit paths to MAX_PATH characters, including the terminating NULL. Unicode versions can handle paths of up to over 32,000 characters if they begin with the special notation "\\?\". GetTempPath() returns the path to the directory for temporary files. It is subject to the same issue regarding potentially returning a path that is too large for the buffer.
APIs	**Function Name** / **Comments** GetLongPathName GetLongPathNameA — ASCII implementation GetLongPathNameW — Unicode implementation GetShortPathName GetShortPathNameA — ASCII implementation GetShortPathNameW — Unicode implementation GetTempPath

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

GetTempPathA	ASCII Implementation
GetTempPathW	Unicode implementation

Method of Attack

Exception Criteria

Solutions

Solution Applicability	Solution Description	Solution Efficacy
When any of the indicated functions are called.	It is a best practice to always size path buffers to MAX_PATH characters. For ASCII usage, this guarantees buffers will be large enough. However, for Unicode usage, with some functions this may not always be sufficient. So should also check to confirm that the size was sufficient. For the functions at issue, if the return value is greater than the buffer size, cchBuffer, call the function again with a buffer that is large enough to hold the path.	Effective.

Signature Details

```
DWORD GetLongPathName(
LPCTSTR lpszShortPath,
LPTSTR lpszLongPath,
DWORD cchBuffer
);
DWORD GetShortPathName(
LPCTSTR lpszLongPath,
LPTSTR lpszShortPath,
DWORD cchBuffer
);
DWORD GetTempPath(
```

	DWORD nBufferLength, LPTSTR lpBuffer);

Examples of Incorrect Code	`TCHAR shortPath[MAX_PATH] = TEXT("C:\\ADIR\\SHORT~1.TXT");`
	`LPCTSTR lpszShortPath = shortPath;`
	`DWORD buffSize = 15; // Buffer is too small`
	`LPTSTR lpszLongPath = (LPTSTR)malloc(buffSize *sizeof(TCHAR));`
	`DWORD result = GetLongPath(shortPath, longPath, buffSize );`
	`/* Might have failed - potential bug if don't check result */`

Examples of Corrected Code	`TCHAR shortPath[MAX_PATH] = TEXT("C:\\ADIR\\SHORT~1.TXT");`
	`LPCTSTR lpszShortPath = shortPath;`
	`DWORD buffSize = MAX_PATH;`
	`LPTSTR lpszLongPath = (LPTSTR)malloc(buffSize *sizeof(TCHAR));`
	`DWORD result = GetLongPath(shortPath, longPath, buffSize );`
	`if (result > MAX_PATH) {`
	`delete lpszLongPath;`
	`buffSize = result;`
	`lpszLongPath = (LPTSTR)malloc(buffSize*sizeof(TCHAR));`
	`if (! GetLongPath(shortPath, longPath, buffSize))`
	`{ handleError(); }`
	`}`

Source Reference	• http://msdn.microsoft.com/library/default.asp?url=/library/en-us/fileio/fs/getlongpathname.asp[2]
Recommended Resources	• MSDN reference for GetLongPathName[3] • MSDN reference for GetShortPathName[4] • MSDN reference for GetTempPath[5]
Discriminant Set	**Operating System**: • Windows **Languages**: • C • C++

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. mailto:copyright@cigital.com